CLAIM AMENDMENTS

Please amend the claims as indicated hereinafter.

1.-28. (Canceled)

29. (Currently Amended) A security system for securing access to an operating system of a computer having at least a host central processing unit (CPU), a memory used by the host CPU to load programs from the operating system in order to operate the computer, a storage device for storing data to be used by the computer; and a chain of components connecting the host CPU to the storage device, the security system comprising:

a security partition formed in the storage device, the operating system of the computer being stored in the security partition; and

a security device comprising a hardware processor or controller for intercepting communications and selectively blocking access to operating system data between the host CPU and the security partition;

wherein the security device is deployed along the chain of components that connect the host CPU to the storage device;

wherein the security device's processor or controller is distinct from the host CPU; and

wherein during operation of the operating system the security device is arranged to: ~~divert and~~ intercept requests to write changes to operating system files in the security partition; in response to the requests, instead of write the changes to the operating system files in the security partition as targeted by the requests, write the changes to a location different than the security partition; ~~so that~~ and cause normal operation of the operating system to continue~~s even though~~ without writing the changes to the operating system files in the ~~secure~~ security partition ~~have not been updated~~.

30. (Previously Presented) The security system as claimed in claim 29, wherein each user of the computer has an associated access profile, each access profile comprising information indicative of the level of access to portions of the storage device permitted by a user, and the security device controlling access to the storage device by a user in accordance with the access profile associated with the user.

31. (Canceled)

32. (Previously Presented) The security system as claimed in claim 29, wherein said security device is independent and separately configurable of said host CPU.

33. (Canceled)

34. (Currently Amended) The security system as claimed in claim 29, wherein the ~~security device is arranged to divert and write operating system files to~~ location different than the security partition is at least a portion of a flash ROM of the security device.

35. (Currently Amended) The security system as claimed in claim ~~33~~ 29, wherein the ~~security system is arranged to divert and write operating system files to~~ location different than the security partition is at least a portion of an invisible partition formed in the storage device.

36. (Previously Presented) The security system as claimed in claim 30, further comprising authentication means for authenticating a user of the computer and associating the user with a prescribed access profile, said security device controlling subsequent access to the security partition in accordance with the access profile associated with the user.

37. (Canceled)

38. (Previously Presented) The security system as claimed in claim 30, wherein said security device is configured to block all access by the host CPU to the storage device before initialisation of the security system, and to selectively permit access immediately after said initialisation in accordance with a respective access profile.

39. (Currently Amended) The security system as claimed in claim ~~38~~ 36, wherein said authentication means enables a software boot of the computer to be effected only after correct authentication of a user, and said security system permits normal loading of the operating system during the start up sequence of the computer following said software boot.

40. (Previously Presented) The security system as claimed in claim 29, wherein said security device is physically deployed between an interface adapter and the storage device within a data access channel of the chain of components connecting the host CPU and the storage device.

41. (Previously Presented) The security system as claimed in claim 39, wherein said security device is integrated in a bridging circuit within the chain of components connecting the host CPU and the storage device or within the storage device.

42. (Currently Amended) A method for securing access to an operating system of a computer, comprising:

forming a security partition in a storage device;

storing the operating system of the computer in the security partition;

loading operating system data from the operating system into a random access memory;

using one or more host central processing units (CPUs)to execute programs in the operating system based on the operating system data loaded into the random access memory;

intercepting communications and selectively blocking access to operating system data between the host CPUs and the security partition at a security device deployed along the chain of components connecting the host CPUs to the storage device, wherein the security device operates independent of the host CPU; and

intercepting, at the security device, requests to write changes to operating system files in the security partition;

~~diverting and~~ in response to the requests, instead of writing the changes to the operating system files in the security partition as targeted by the requests, the security device writing the changes to a location different ~~to~~ than the security partition; ~~during operation of the operating system so that~~ and

the security device causing normal operation of the operating system to continue~~s even though~~ without writing the changes to the operating system files in the ~~secure~~ security partition ~~have not been updated~~.

43. (Previously Presented) The method as claimed in claim 42, further comprising associating each user with an access profile comprising information indicative of the level of access to portions of the storage device permitted by a user; and

for each user, selectively blocking access between the host CPU and the security partition in accordance with the access profile defined for the user.

44. (Canceled).

45. (Previously Presented) The method as claimed in claim 43, further comprising authenticating a user of the computer, and associating the user with an access profile after successful user authentication.

46. (Previously Presented) The method as claimed in claim 42, wherein said selective blocking comprises controlling access between the host CPU and the security partition independently of the host CPU.

47. (Previously Presented) The method as claimed in claim 42, wherein said selective blocking comprises totally blocking access to the storage device by the host CPU during initialisation of the computer, and intercepting all said access immediately after said initialisation and before loading of the operating system of the computer.

48. (Previously Presented) The method as claimed in claim 45, including performing a software boot of the computer only after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer after said software boot.

49. (Canceled)

50. (Currently Amended) The method as claimed in claim 42, wherein the ~~operating system files are diverted and written to~~ location different than the security partition is at least a portion of a flash ROM in the security device.

51. (Currently Amended) The method as claimed in claim 42, wherein the ~~operating system files are diverted and written to~~ location different than the security partition is at least a portion of an invisible partition formed in the storage device.

52. (Previously Presented) The method as claimed in claim 42, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

53. (Previously Presented) The method as claimed in claim 42, wherein the security device is a dedicated hardware device comprising a dedicated CPU for processing the intercepted communications and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition.

54. (Previously Presented) The method as claimed in claim 42, wherein the security device is integrated into a bridging circuit comprising logic for processing the intercepted communications and, based on the intercepted communications, determining whether to block data access between the host CPU and the security partition.

55. (New) The system of Claim 30, wherein the security device is arranged to divert to the scratch location write operations to the security partition requested by a first user, but permit performance of write operations to the security partition requested by a second user.

56. (New) The system of Claim 30, wherein the security device is further configured to erase the changes written to the scratch location without the changes having been written to the operating system files targeted by the requests.

57. (New) The method of Claim 42, further comprising diverting to the scratch location write operations to the security partition requested by a first user, but permitting performance of write operations to the security partition requested by a second user.

58. (New) The method of Claim 42, further comprising erasing the changes written to the scratch location without the changes having been written to the operating system files targeted by the requests.